

SonicWALL / Aventail Connect Tunnel Service 10.6 User Guide

SonicWALL® ECLASS

SonicWALL Aventail Connect Tunnel Service

The Connect Tunnel client is a Windows client component of the SonicWALL Aventail E-Class Secure Remote Access (SRA) solution that enables secure, authorized access to Web-based and client/server applications, and to Windows file shares.

In a server environment, you can install and configure an add-on component—Connect Tunnel Service—so that the VPN connection starts automatically without user intervention: no user login is required, and no user interface or icons are displayed. For example, you may want to synchronize data between a remote system in the field and a file server secured behind the VPN at corporate headquarters. On the remote system—running the Windows Server platform—Connect Tunnel Service is configured to run at a specific time, connect to the corporate file server, and synchronize its database with the master database at headquarters.

Installing Connect Tunnel Service

Using the Connect Tunnel Service involves installing both Connect tunnel and Connect Tunnel Service.

► To install and configure Connect Tunnel Service

1. On the **Client Installation Packages** page in AMC (**Agent Configuration > Download**), download the 32-bit or 64-bit installation packages for both the Connect tunnel and Connect Tunnel Service (the <xx> in the filename represents the language you selected).
2. Install Connect tunnel first (*ngsetup_<xx>.exe* or *ngsetup64_<xx>.exe*). A shortcut named *Aventail VPN Connection* is created on the desktop.
3. Install Connect Tunnel Service (*ctssetup_<xx>.exe* or *ctssetup64_<xx>.exe*). A shortcut named *Aventail VPN Service Options* is created on the desktop.

4. On the desktop, double-click the *Aventail VPN Service Options* shortcut. Alternatively, double-click **Aventail VPN Service Options** in the Control Panel. The **Aventail VPN Service Properties** dialog box appears.

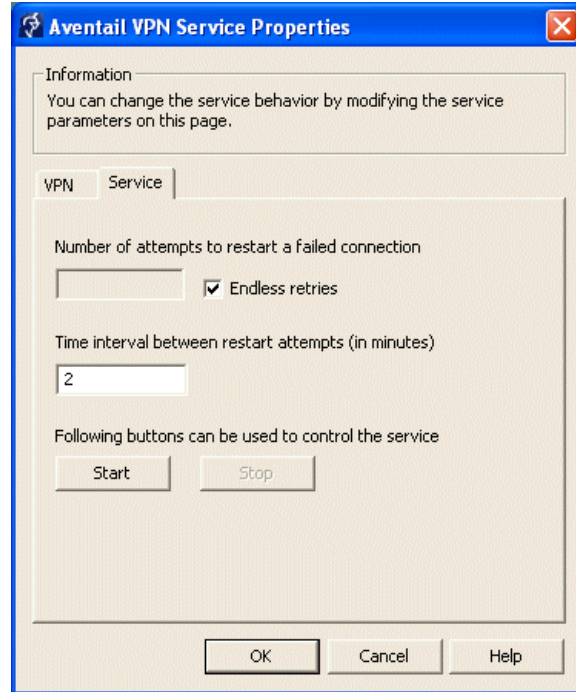
5. On the **VPN** tab, configure these settings:

Setting	Description
VPN Connection Name	Type the name of the Aventail Connect client connection object exactly as it appears in the Windows Network Connections window (Start Connect To Show All Connections). By default, this is Aventail VPN Connection.
Hostname or IP address	Type the host name or IP address of the SonicWALL Aventail E-Class SRA appliance to log in to.
Login group	Type the name of the realm to log in to.
Username and Password	Type the credentials for a user in this Login group (realm). You must enter a username and password or a certificate CN. In some cases of chained authentication, both a username and certificate are required.
Certificate CN	A certificate's common name (CN) identifies its owner. Specify the CN for the certificate associated with this realm.

6. On the **Service** tab, configure the following settings:

Setting	Description
Number of attempts to restart a failed connection	Specify how many times to attempt restarting if an initial connection attempt fails.
Time interval between restart attempts	Specify the amount of time (in minutes) to wait between restart attempts.

- Click the **Start** and **Stop** buttons to control the service.



- To verify that Connect tunnel started, open the *Aventail VPN Connection* shortcut on the desktop. You should see the established connection. Alternatively, you can issue the `ipconfig` command on the command line to verify that you have a virtual IP address for the Aventail VPN Connection.

Importing the Client Certificate

The certificate specified for Connect Tunnel Service must be located in the *Local Computer* certificate store of the user's device; certificates in a user's store are not available to the service. The Microsoft Management Console (MMC) is a tool for managing administrative tools, including snap-ins and extension snap-ins.

► To import a certificate into the user's *Local Computer* store

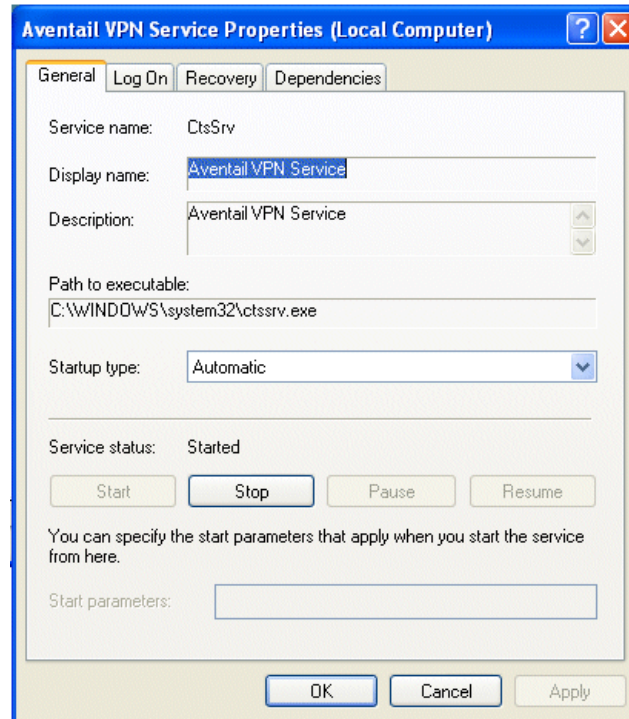
- To open the Microsoft Management Console, click **Start**, and then click **Run**. Type `mmc` in the **Open** box.
- In the **File** menu, choose the option for adding a snap-in.
- To add a standalone snap-in, click **Add**, and then click **Certificates**.
- Snap-ins can manage certificates for different accounts; select **Computer account**, and then select **Local computer**. You should now see *Certificates (Local Computer)* in the list of standalone snap-ins.
- The certificate must now be copied to a certificate store. In Microsoft Management Console, right-click *Personal*, and then select **All Tasks > Import**.
- Specify the certificate file you want to import, along with its password.
- Place the certificate in your *Personal* store.

Using Windows Services to Run Connect Tunnel Service

You can use Windows Services to manage Connect Tunnel Service on a local or remote computer.

► How to use Windows Services to configure and run Connect Tunnel Service

1. On the Windows Server platform running Connect Tunnel Service, run Windows Services and open the Aventail VPN Service Properties dialog box (**Control Panel > Administrative Tools > Services > Aventail VPN Service**).



2. Use these settings to control the service (start, stop, pause, resume, or disable it), set up recovery actions in case of service failure, or disable the service for a particular hardware profile.

Using a Command or Script to Run Connect Tunnel Service

You can use the Windows `sc.exe` utility to communicate with Service Controller (`services.exe`) from the command prompt or in a batch file. This enables you, for example, to automate the startup and shutdown of the Aventail VPN service. Or, in an environment where you want users to be able to start the VPN connection by clicking on a shortcut (and without being aware of the credentials), you could also create a shortcut on the desktop that launches a command or batch file.

For example, start and stop the service on a remote computer with the following commands:

```
sc \\SERVERNAME start ctssrv
```

```
sc \\SERVERNAME stop ctssrv
```

To start or stop the Connect Tunnel Service from the command line or a third-party application, invoke these commands:

```
%windir%\system32\sc.exe start ctssrv
```

```
%windir%\system32\sc.exe stop ctssrv
```

Troubleshooting

Use the Windows Event Viewer (**Control Panel > Administrative Tools > Event Viewer > Application**, where the **Source** is "CTS") to view any information, warning, or error messages related to running Connect Tunnel Service. For more detailed messages, look in the service log (the default location is %ALLUSERSPROFILE%\Application Data\Aventail).

Notes

- If your environment includes an outbound HTTP proxy for access to the Internet, you must use one that does not require authentication, otherwise you will see the following error message in the log file for Connect Tunnel Service (*ctssrv.log*): "Direct internet access is not available." You must also configure Connect Tunnel Service to run under a Windows user account with administrative privileges.

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124

T +1 408.745.9600 F +1 408.745.9300

www.sonicwall.com



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™



©2011 SonicWALL and the SonicWALL logo is registered trademarks of SonicWALL, Inc. Dynamic Security For The Global Network is a trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. 06/10 SW 996

232-002045-00 Rev A
10/2011